Chapter 1 Departmental/Agency Strategic Business Initiatives and Major Business Requirements

Agency Mission Statement

The Office of the State Auditors mission is to provide state agencies, the legislature and the people of North Carolina with professional, independent evaluations of the State's fiscal accountability and public program performance. We continually strive to ensure that our state government executes its management responsibilities in compliance with applicable laws, rules, regulations, and policies. We also evaluate management controls and policies in an effort to assist state agencies in making more efficient and effective use of public resources.

A. Major Business Initiative – Audit Watch

In today's environment, as legislators and taxpayers scrutinize expenditures and search for increased value for hard-earned tax dollars, technical excellence and timely reports are not enough. OSA must provide audits in the most efficient manner, and we must dramatically change the way audits are conducted. What's the goal? Improve efficiency and effectiveness without sacrificing quality.

Our potential for major productivity gains largely resides in the skills and attitudes of our people. As a result, our auditors need to continuously seek ways to eliminate inefficiencies and efforts that don't add value. To succeed, they must be adequately trained and work in a culture that promotes and rewards this behavior.

To reach these goals OSA will be engaging Audit Watch Inc., a group who specializes in the design, training, and implementation of change programs for accounting firms, to lead this project. OSA has the unique opportunity, with Audit Watch's assistance, to prove gains public accounting firms have achieved can be duplicated or even improved on by government entities.

Anticipated Benefits:

- Improved Efficiency
- Enhanced Client Service to Legislators and Citizens
- Improved Audit Quality
- Higher Staff Morale

B. Other Strategic Business initiatives and Major Business Requirements

1. To provide accurate and timely reporting of NGO compliance issues and reports.
2. To publish and distribute audit reports and news releases in a timely fashion that is consistent with both OSA policy and NC State law.
3. To provide timely and accurate information and resources to OSA employee's in an easy to use and secure manner.

Chapter 2 – Requirements for Transitioning Existing IT Activities/Resources

A. Current Projects

1. Data Warehousing - SAS

This project will replace and enhance the current NGO application (see 2.B.2). In addition, it will serve as a foundation for future business analysis (BA) and business intelligence (BI) applications.
OSA needs to coordinate and analyze data from disparate sources to better understand and to pull additional information from the States financial workings.

2. Network Performance Monitoring Services

Network monitoring tool proposed by ITS to monitor network traffic and application response. The primary objective is to gain visibility of network bandwidth and diagnostic ability on application response time

3. Beacon

To consolidate OSA Human Resource procedures, specifically employee payroll, with statewide systems and procedures

4. SARA – E Partners

The Office of the State Auditor (OSA) has for well over a decade, utilized a static-pages website as an intranet to provide a presentation for its internal information. This top-level intranet website is named "SARA" (State Auditors' Resource Area). OSA proposes an intranet website rebuild project to Senior Design Team of North Carolina State University. (E-Partners)

B. Applications

1. Electronic Publishing System (EPS)

The Electronic Publication System allows interested parties to sign up for reports that meet their selection criteria. Audit reports are automatically distributed to registered users when released.

Minor enhancements to improve efficiency and accountability are planned for the EPS system. In addition, enhancements may be required to integrate EPS with the State Auditors Resource Area (SARA) project.

2. Non Governmental Grants Compliance Application (NGO)

OSA is responsible for receiving reports from Non-governmental Organizations (NGO) receiving State grants. The NC General Assembly required OSA to make a determination as to whether a Grantee is in compliance with reporting requirements, as well as verifying that audits are performed and that the review of

those audits is in compliance to standards for grantees receiving $500,000 or above.

The NGO application will be maintained until it is successfully replaced by direct outputs of the Data Warehousing SAS project.

3. Remote Deployment of Desktop Services (Remote)
Remote Deployment of ACL and AS2 utilizing WINbatch and patch link server. ACL and AS2 are mission critical vendor supplied applications for performing audits.

The Remote Deployment of Desktop Services will be maintained into the foreseeable future.

4. Time Reporting System (TRS)
Application provides time reporting and management for all OSA employees and provides billing information for cost recovery.

The TRS system will be maintained until it is enhanced by or replaced by the Statewide Beacon HR/Payroll initiative.

Application Roadmap

	2005	2006	2007	2008	2009	2010	2011
EPS	Enhance	Enhance	Enhance	Enhance	Enhance	Enhance	
NGO	Maintain	Maintain	Maintain	Maintain			
TRS			Maintain	Maintain	Maintain	Maintain	
Remote	Maintain	Maintain	Maintain	Maintain	Maintain	Maintain	Maintain

C. Infrastructure Assets

1. Refresh older computers and infrastructure with up to date technology.
2. Completely rework of all external OSA network traffic to conform to ITS policy while enabling end to end data encryption to ensure data integrity.
3. Replace aging and unsupported network switching infrastructure (Nortel Switches)
4. Microsoft Enterprise Agreement / Server Software Refresh
    a. Replace/refresh existing Microsoft office, productivity and server software to ensure standardization, maintain compliance and ease administrative and support issues. These include:
        i. Enterprise Server – Refresh OSA MS Enterprise Server
        ii. Exchange Server – Refresh OSA Exchange Server
        iii. Install and configure SharePoint server in support of SARA project
        iv. SQL Server – Refresh SQL server

v. MS Office - Refresh office and productivity software to latest versions from Microsoft.

5. Improve wireless networking security to provide both offensive and defensive network security.
6. To improve communications with auditors who are working in the field via VoIP and "follow me" phone access.
7. Improve computer security for field auditors by providing data center access to critical applications so that in event of theft or loss data will not be compromised.

D. Operations/IT Management

1. Move towards an ITIL based, service orientated IT organization
2. Improve Project Management and Delivery (UMT PPM Tool)
3. Improve Applications Portfolio Management (UMT APM Tool)
4. Improve Infrastructure assets management and inventory control (IWise)
5. Internal agency consolidation plans and progress in preparation for statewide consolidation of infrastructure assets
6. Improve Security management by implementing a network monitoring tool to monitor network traffic and application response.
7. Improve Disaster recovery and business continuity planning (LDRPS Software)

E. Human Resources

MIS Staff

CIO (Lenny Superville, Phd Applied Math Operations Research /Industrial Engineer)
Technology Support Analyst (Michael Fetting)
Technology Support Specialist (Leo Alls)
Business and Technology Applications Analyst (Neelema Chitoor)
Business and Technology Applications Specialist (Mark Smith)
Business and Technology Applications Specialist (Gary Hinkel)
Network Specialist (Paul Saksa)
Intern
NC State Senior Design Team (E-Partners)

Chapter 3 – IT Specific Economic-Driven Requirements or Opportunities

IT Specific economic-driven requirements or opportunities

1. To modify OSA IT systems, resources, policies and procedures so they conform to industry best practices as detailed in the Information Security Assessment produced for OSA by Symantec.
2. To adjust salaries for IT professionals to correct imbalance between current actual salaries and recommended salary targets as outlined by career banding.

Chapter 4 – IT Initiatives Developed From and Aligning With Plan Drivers

Initiative: Non-Governmental Organizations	**Primary Plan Driver: 2.B.2** (Current Applications – NGO) **Priority: 1**
Summary	OSA is responsible for receiving reports from Non-governmental Organizations (NGO) receiving State grants. The NC General Assembly required OSA to make a determination as to whether a Grantee is in compliance with reporting requirements, as well as verifying that audits are performed and that the review of those audits is in compliance to standards for grantees receiving $500,000 or above. One purpose for this report is to provide timely information to grantor agencies on NGOs which have failed to comply with reporting requirements. Under administrative rules which became effective in July of 2005, grantor agencies may withhold subsequent allocations to organizations who fail to comply with reporting requirements.
Objectives	• For Grant Compliance and Reporting, a real-time online system needs to be developed • A Seminar Registration system (SRS) will be built. This will maintain/support online course materials, provide an online registration system, track CPU's as well as give OSA the capability to offer online courses such as Web casts • This framework site will host all the existing static information, and it will have links to the SRS application as well as the Grant Compliance application. • An ad-hoc reporting/ data mining component to the system is needed to investigate possible compliance issues and to identify trends not inherently apparent. In addition, future connections to the State HR/Payroll system are envisioned.
Time Frame	First quarter 2007
Agency Relationships	Plan Driver:1.A (Audit Watch – office efficiency) Plan Driver: 1.B.1 (Improve NGO reporting) Plan Driver: 2.A.1 (Current Projects - Data Warehousing – SAS) Plan Driver: 2.A.4 (Current Projects - SARA E-Partners)
Statewide Relationships	Funds for this project are coming from OSC and the Beacon Enterprise Data Warehouse Initiative.
Resources Involved	HR: Business and Technology Applications Specialist Professional Contract Services
Costs	Professional Services: $112000 Training: $20000 Subscription Services: $50000 Project Management Services: $38000 Hosting at ITS: $30000 TOTAL: $ 250000

Initiative: Data Mining/ Business Intelligence	**Primary Plan Driver: 2.A.1** (Current Projects – Data Warehousing) **Priority: 2**
Summary	As NC State Government moves to a shared IT infrastructure (driven by SB 991) it is imperative that critical systems to ensure that the foundations for business intelligence and business analysis are put in place.
Objectives	• To assist ITS in developing Data Warehousing and Shared Data Services for all of NC State Government
Time Frame	Fiscal Year 2007
Agency Relationships	Plan Driver 2.A.3 (Beacon Project) Plan Driver: 2.B.2 (Applications – Non Governmental Grants)
Statewide Relationships	Statewide Beacon Project
Resources Involved	HR: Business and Technology Applications Specialist
Costs	$20000 – Training and staff development $20000 (primarily as a portion of resource use –tasks and their completion will be considered as regular and expected duties.)

Initiative: Infrastructure Upgrades (Nortel Switches)	**Primary Plan Driver: 2.C.3** (Infrastructure Assets – Switch Replacement) **Priority: 3**
Summary	In early 1997, Nortel began shipping a core networking product called the Accelar 1200. This product along with other Nortel products distributed throughout the Auditor building became the core foundation for the data networking infrastructure. While these products have been extremely reliable for the last 9 years, their lifecycle has ended. The ITS standard for updating this type of equipment is a much shorter 5 years. On November 30th, 2006 the Accelar 1200 product will not have a support option available from Nortel. This means that if there is a failure of hardware or software on the product, significant downtime is likely. Nortel proposes that the N.C. State Auditor updates the equipment in the network to avoid this downtime as well as make security enhancements to the network infrastructure.
Objectives	• Replace outdated Nortel Switches • Increase security on all internal networks up to port level inspections. Currently two options are being considered: *Option 1:* Replace the core Accelar 1200 with 2 Nortel ERS5530 switches. Replace the Baystack 450 switches in the closets with Nortel ERS5510 switches. Provide dual fiber paths from each of the closets distributed across the core ERS5530s. Put in place a Nortel technology called Split Multi-Link trunking (SMLT) at the core. *Benefits:* No Single Point of Failure in the Network means 99.999% uptime. Nortel has provided for redundant fiber connections from each closet in the building back to the core closet. This means that any fiber module or physical pair of fiber

	itself from any closet can have a failure and the network stays operational. Closet switches are connected together in a fashion we call "resilient stacking". This means that if any switch in a stack has an outage, only the users on the ports on that switch are affected. The rest of the users on the network are not affected. In addition, Nortel is splitting the connections from each closet across 2 core switches utilizing a technology called SMLT. As networks grow ever more critical, there is an increasing demand for multiple paths from all wiring closet switches into the core of the network to eliminate all single points of failure. Nortel's SMLT technology allows for no single point of failure on the network. Some vendor solutions utilize an aging protocol called Spanning Tree to provide network redundancy. Spanning Tree only allows for one link from each closet to be active at any one time. SMLT allows for both links to be active, doubling throughput. In case of a network outage of either core switches, SMLT allows for the network to failover in less than 1 second (average time is 0.4 seconds). Spanning tree fails over in at least several seconds. This type of delay would be enough to frustrate users using real time media (voice or video) and could be long enough to reset IP phones. Minimizing down time during scheduled network maintenance, such as system upgrades or configuration changes, is also a key requirement of today's networks. Providing network operators with tools that allow them to apply network changes during working hours, rather than after hours, can lead to significant cost savings over time. The Nortel SMLT solution provides a simple way of upgrading aggregation/core devices without impacting overall network availability. Increasing the speed of the network means more productivity. Using SMLT technology, Nortel can double the bandwidth from each closet (1GB to 2GB) to the core of the network resulting in higher throughput. In addition, the switches used in this design are 10 times faster than the switches N.C. Auditor is using today. Security is in the DNA. Security enhancements are inherent to the products. Better security means secure information won't be compromised. Nortel has features built into the solution that provide for enhanced security over what is currently used. Features like SSHv2, 802.1x, and SNMPv3 are standard in Nortel's products. Having the latest technology means N.C. Auditor can support even more enhanced security features both now and in the future. *Option 2:* Add Power over Ethernet Capabilities Power over Ethernet (PoE) technology provides power and data connectivity to devices such as IP phones, wireless access points, network cameras, security and lighting devices, and access control devices (i.e. badge readers). According to IDC's Worldwide Power over Ethernet 2004-2008 Forecast and Analysis report, the Power over Ethernet market revenue is expected to grow at an 8.9 percent CAGR (compound annual growth rate) over the next five years. Benefits: Purchasing this capability now means you'll avoid costly retrofitting later. Many network devices are becoming powered over Ethernet cable instead of through power outlets (wall outlets). If N.C. Auditor believes at some point that technologies listed above will be used in the network, purchasing PoE switches will avoid costly retrofitting of network devices later. In addition, NC Auditor will have these capabilities from day 1, which will make the time to roll out new services shorter. Retrofitting devices for PoE later means adding points of failure in the network. Additional points of failure means downtime and loss of productivity. If NC Auditor must retrofit for PoE capabilities later, either powered patch panels or PoE injectors must be used. This will add multiple points of failure into the network which inevitably will result in downtime and loss of productivity.

	Add-On capabilities: Endpoint Security: Adding Nortel's Secure Network Access (NSNA) means NC Auditor can verify key attributes of every device on the network to protect assets at the most vulnerable point of entry – the network edge. A key element described in the Nortel Layered Defense posture is endpoint security. The network edge is no longer where the corporate firewalls are. A paradigm shift has pushed the network edge to where the user and their computing device are located. The road warrior connecting to the corporate network can have secure remote access to your network. Organizations are extending their firewall to the corporate network to increase protection for critical computing resources such as data centers and mission-critical applications. According to ESG Research 2005 report, 43% of survey correspondents confirmed that their Internet worms/virus had been "carried in on an employee laptop". Securing these devices is integral to the defensive posture as most enterprises have more users than servers. Critical to managing these systems are security policies specifying enterprise configurations. Security policies include antivirus software, personal firewall software and enterprise configurations, such as disallowing noncompliant network applications. Controlling what devices are permitted to connect to the network provides significant protection. Does an enterprise really know what is connected to their network? Enterprise-provided systems, employees' personal devices, contractors, consultants and vendor support personnel all have devices which may be connected at any given time. Limiting network access to only authorized systems is essential. Nortel SNA addresses endpoint security, and implements automated configuration and security policy enforcement, increasing access control and risk mitigation. Nortel SNA, featuring our Tunnel Guard technology, checks to ensure the latest anti-virus, firewall applications, or software patches are running before authorizing users. All system elements can be evaluated including the operating system, patches, anti-virus software, personal firewall status, registry settings and other components. Verifying compliance and blocking connections from non-compliant systems can provide 100 percent compliance with corporate policy. Threat Protection: If there is vulnerability in the network, NC Auditor needs to know about it as soon as the threat is detected so the threat can be mitigated as soon as possible so key assets are not compromised. Nortel's Threat Protection System (TPS) detects, reports, blocks, and reports on any security event in the network.
Time Frame	First quarter 2007
Agency Relationships	Plan Driver: 2.A.2 (Current projects – network performance monitoring) Plan Driver: 2.C.2 (Infrastructure Assets – ESAP) Plan Driver: 2.C.6 (VoIP)
Statewide Relationships	
Resources Involved	HR: Network Specialist Nortel Support Services *See Attachment: Nortel Replacement*
Costs	Total Solution (Hardware+Services): $180756 Total Recurring Maintenance: $14406 *See Attachment: Nortel Replacement*

Initiative: Software/Server Infrastructure Refresh/Upgrade (MS Enterprise Agreement)	**Primary Plan Driver: 2.C.4** (Infrastructure Assets – MS Enterprise Agreement) **Priority: 4**
Summary	Enter into an Enterprise Agreement with Microsoft for all MS Operating Systems, Office applications and Servers. This includes: Office Pro, Windows Pro, Windows Server CALS, Exchange Server CALS, Systems Mgmt CALS, Share Point Server CALS. SQL Server, Exchange Server. *See Attachment: Microsoft Proposal*
Objectives	• Improve security • Mitigate risks of aging technology • Enable improvements of operations inherent in enhanced server technologies • Reduce Total Cost of Ownership (23%-35% cost savings compared to Select purchasing) • Ease of Administration • Standardization/Maintain Compliance
Time Frame	Fiscal Year 2007
Agency Relationships	Plan Driver 1.A (Audit Watch – Improved office efficiency) Plan Driver 2.B.1 (Current Applications – EPS) Plan Driver 2.B.2 (Current Applications – NGO) Plan Driver 2.B.4 (Current Applications – TRS) Plan Driver 3.1 (Information Security Assessment updates)
Statewide Relationships	
Resources Involved	HR: Technology Support Specialist HR: Network Specialist HR: Business and Technology Applications Specialist
Costs	Netware $500 Microsoft Enterprise Agreement pricing (3-year agreement) $181457 *See Microsoft Costs for year by year breakdown* $15000 (primarily as a portion of resource use –tasks and their completion will be considered as regular and expected duties.)

Initiative: Security/ Business Continuity Specialist	**Primary Plan Driver: 2.D.7** (Operations/IT Management – Improved DR and BCP) **Priority: 5**
Summary	As a result of BCP requirements outlined in NC State Statue 147-33.89 and Executive Order #102 , OSA intends to develop a position to review, maintain and implement policies and procedures for the security of the OSA IT Infrastructure and Disaster Recover/Business Continuity planning. This position would represent the increase in resources devoted to the information security program to ensure that all operational details are adequately covered on an ongoing basis recommended by Symantec in their Information Security Assessment.

Objectives	• Improve security • Improve IT Policy to ensure alignment with statewide (ITS) and industry best-practice • Improve OSA's ability to develop comprehensive business continuity plans
Time Frame	Fiscal Year 2007
Agency Relationships	Plan Driver 2.C.5 (Infrastructure Assets – Improved wireless security) Plan Driver 2.C.6 (Infrastructure Assets – Improved communications via VoIP) Plan Driver 2.C.7 (Infrastructure Assets – Improved Security for Field Auditors) Plan Driver 2.D.1 (Operations/IT Management – ITIL) Plan Driver 2.D.4 (Operations/IT Management – Internal Agency Consolidation Plans) Plan Driver 2.D.6 (Operations/IT Management – Improved Security via network monitoring) Plan Driver 3.1 (Information Security Assessment updates)
Statewide Relationships	General Statute 147-33.89 (Business Continuity Plan) Executive Order 102 (Continuity of Operations Plan)
Resources Involved	HR: Network Specialist HR: Business and Technology Applications Specialist
Costs	$100000 (Anticipated salary + support systems required) OSA intends to investigate possible use of Homeland Security grants and funds for this position.

Initiative: IT Salary Adjustment	**Primary Plan Driver: 3.2** (Salary Adjustments) **Priority: 6**
Summary	There is currently an imbalance between salary requirements for IT staff as outlined by career banding and the actual salary being paid to IT staff. This initiative is to make necessary appropriations to correct that imbalance.
Objectives	• Improved ability to retain valuable employees • Improved ability to attract new hires for IT positions
Time Frame	Fiscal Year 2007
Agency Relationships	Plan Driver 1.A (Audit Watch – Improved office efficiency)
Statewide Relationships	
Resources Involved	OSA Human Resources
Costs	$100000

Initiative: AirDefense (Wireless Security)	**Primary Plan Driver: 2.C.5** (Infrastructure Assets – wireless security) **Priority: 7**
Summary	Though much time, money and effort has been spent to protect against threats on the wired side of the network, wireless devices represent a vulnerable "back door" for intrusions. Any device which ties into a wireless network can be leveraged to hack into the wired network. Unless fully protected, wireless-enabled PC's can be probed or spoofed at work, home, in airports and at wireless hot spots. Clearly, Enterprise security policy must address the issue of ongoing malicious threats.

	To mitigate legal and regulatory risks, policies can be enabled to prevent employees from accidental wireless association with other near-by businesses. The AirDefense solution is utilized to implement and enforce wireless network policy, maintain continuity, monitor activity and take action. The AirDefense solution provides proactive wireless intrusion prevention through simultaneous policy enforcement on both RF airspace and wireless-enabled PCs. All wireless networks face the following threats: • Rogue Devices that provide unsecured access to both wired and wireless network • Associations, whether they are accidental, malicious, or peer-to-peer. • Intruders or hackers that can launch attacks (DoS, Identity Theft) • Bridging wireless laptops can create new exposures to hackers • Wireless Phishing can hijack users at hotspots (AirSnarf, Hotspotter, Evil Twin) As enterprises become increasingly dependent on data networking and wireless connectivity for enhanced productivity, such attacks become more sophisticated and more prevalent.
Objectives	• Full time (24x7) monitoring of NC Auditor 802.11 a/b/g air space to identify security and performance issues • Advanced WLAN attack detection and mitigation • Prevention of WLAN security breaches • Enhanced wireless network performance monitoring and diagnostics • Detection of all rogue devices such as access points (APs) and stations (laptops, scanners, PDAs) and legally terminate at client discretion • Notify when NC Auditor laptops/computers connect to non-company APs • Disconnect NC Auditor devices if connected to non-NC Auditor AP by accident • Analyze security incidents (e.g., when a rogue is detected, who it connected to, how long it was connected, and how much data was transferred) • Reporting: Provide audit trail and forensics of all attempted and potential wireless security incidents—important for policy refinement • Protection of remote workers from wireless intrusion • Uniform wireless policy formulation and enforcement • Wireless security skills development for NC Auditor staff • Formal wireless security training/certification
Time Frame	Fiscal Year 2007 OSA will use a 2-phased approach that includes a pilot of 2 of the WIPS solutions in the AirDefense portfolio of products—AirDefense Enterprise and AirDefense Personal—followed by the larger deployment to the field and inclusion of the product Phase One will provide WIPS coverage for the Customer's headquarters location in Raleigh. Phase Two will provide WIPS coverage at remote locations during state audit services delivery.
Agency Relationships	Plan Driver 2.C.7 (Infrastructure Assets – Improved security for field auditors) Plan Driver 2.D.6 (Improve security management) Plan Driver 3.1 (Information Security Assessment updates)
Statewide	

Relationships	
Resources Involved/ Costs	HR: Network Specialist *See attachment AirDefense Proposal*
Costs	Phase 1: $23033 Phase 2: $86215

Initiative: ESAP and OSA End to End Encryption	**Primary Plan Driver: 2.C.2** (Infrastructure Assets - ESAP) **Priority: 8**
Summary	Total reworking of all external OSA network traffic. End to end encryption is an OSA defined model for data privacy to allow auditors to give unqualified opinions no matter what network their data travels through. It involves or includes data security if a laptop is stolen or a network communication is intercepted.
Objectives	• Comply with ITS mandate while maintaining OSA data integrity and privacy. • End to end encryption for OSA data privacy and security through the Internet and ITS controlled networks.
Time Frame	First quarter 2007
Agency Relationships	Plan Driver 2.C.1 (Infrastructure Assets – Field Auditor Security) Plan Driver 2.C.3 (Infrastructure Assets – Switch replacement)
Statewide Relationships	ESAP is a statewide networking infrastructure update sponsored and coordinated by ITS
Resources Involved	HR – Network Specialist
Costs	Disk Encryption for all OSA field laptops - $7500 FIPS compliant Application Level Encryption - $39154 Secure Enterprise Consulting charges - $4500 Softboot software - $25000 Server for Softboot - $18000 TOTAL: $94154

Initiative: Vital Services Suite	**Primary Plan Driver: 2.A.2** (Current Projects – Network Monitoring) **Priority: 9**
Summary	Network monitoring tool proposed by ITS to monitor network traffic and application response.
Objectives	• to gain visibility of network bandwidth and diagnostic ability on application response time • improve and increase network efficiency • improve network security
Time Frame	Fiscal Year 2007
Agency Relationships	Plan Driver 2.C.3 (Infrastructure Assets – Switch Replacement) Plan Driver 2.D.6 (Operations/IT Management – Improved Security) Plan Driver 3.1 (Information Security Assessment updates)

Statewide Relationships	ITS Deployment of Vital Services Suite
Resources Involved	HR: Network Specialist
Costs	$35000

Initiative: State Auditors Resource Area (SARA)	**Primary Plan Driver: 2.A.4** (SARA E-Partner) **Priority: 10**
Summary	The Office of the State Auditor (OSA) has for well over a decade, utilized a static-pages website as an intranet to provide a presentation for its internal information. This top-level intranet website is named "SARA" (State Auditors' Resource Area). *Problems* -Links mainly to documents on external file servers, so these links break frequently. -Few users recruited or trained to keep links and presentation up-to-date; content maintenance more and more frequently falls on MIS staff. -SARA website is not self-maintaining; information owners cannot or do not update their content. Content is out-of-date or does not expire. -SARA has no portal features: -There is no searching, categorization or metadata capability for all of SARA content. -There is no comprehensive, self-maintaining site map. -There is no notification mechanism (alerts or subscriptions). -There is no mechanism to target items to specific users or categories of users (audiences). -There is no document management or team collaboration features. -There are no discussion board or survey capabilities. -There is no anonymous communication path to secure a writer. -SARA content exists on both Windows and Novell volumes, and the security built into the Novell file hierarchy can't be integrated well into a Windows web application or a Windows-based portal. It would be better for more content to reside on Windows servers and portal and to utilize the OSA's Active Directory user / group accounts and security roles. -A lot of collaboration is done on the Novell file server (S: drive) which is not even implemented in SARA. The S: drive folder hierarchy is deep and complex, which makes it difficult for workgroups to find information.
Objectives	• The primary objective of the SARA Portal Project is to implement a portal solution to replace the static web pages of SARA. The OSA would implement the portal using Windows SharePoint Services (WSS) and Microsoft SharePoint Portal Server 2003 (SPS), leveraging objects, properties, and security information from our Windows Active Directory, and content from SARA and the Novell S: drive file share. • The second major objective of the SARA Portal Project is to make the portal-based SARA content both self-maintaining and easily modifiable. Little or no content update efforts should be required of the OSA MIS staff, and at the same time the portal should allow for the inclusion of new resources and currently unrecognized enhancements in an easy and straight forward manner. The project team and OSA MIS staff should work jointly to Identify all the content owners along with the particular content for which they are responsible; Familiarize these content owners with the

	portal implementation; Train and encourage content owners to use the portal interface to maintain and update their information. Recruit volunteers who can provide feedback during the portal implementation process. Content owners must be "conditioned" to use Microsoft Office to connect to the appropriate SharePoint area, list, or document library when editing or saving documents and list items, instead of relying on file server shares and file browsing. We want to move collaboration users into the web-based mechanism for sharing information, and away from the pain of searching and browsing for files in a file hierarchy. • The third major objective of the SARA Portal Project is to implement beneficial portal technology features not available in old static web pages. • A fourth major objective of the SARA Portal Project is to introduce to OSA users the concept and methods of shared user-maintainable websites and collaboration via web pages, and to successfully seed a modernizing change in the organization's approach to sharing information.
Time Frame	Work on this project will be completed in the first semester of the 2006 academic year. (August 2006-December 2006)
Agency Relationships	Plan driver 1.A (Audit Watch – office efficiency) Plan driver 1.B.3 (Improve office communications) Plan driver 2.C.4 (Infrastructure Assets –MS Enterprise Agreement)
Statewide Relationships	
Resources Involved	HR- Project will be designed and developed by NCSU Senior Design team (E-Partner Program) Business and Technology Applications Specialist Business and Technology Applications Analyst
Costs	E-Partners -$5000 Sharepoint Portal hardware, software and licenses - $ 19050 TOTAL: $ 24050

Initiative: Cisco Support	**Primary Plan Driver: 2.C.3** (Infrastructure Assets - Replace aging Infrastructure) **Priority: 11**
Summary	To provide the needed support for existing Cisco products (Firewalls, Access Points, ACS Server Software and Concentrator). (Cisco Smartnet Support Contract)
Objectives	Mitigate risks involved with infrastructure failure
Time Frame	Fiscal Year 2007
Agency Relationships	Plan Driver: 2.C.2 (Infrastructure Assets – ESAP) Plan Driver 2.D.6 (Operations/IT Management – Improved Security via network monitoring) Plan Driver 3.1 (Information Security Assessment updates)
Statewide Relationships	
Resources	HR: Network Specialist

Involved	
Costs	$12220.00(1 year support)

Initiative: Terminal Services	**Primary Plan Driver: 2.C.7** (Infrastructure Assets – Improved security for field auditors) **Priority: 12**
Summary	The North Carolina Office of the State Auditor would like to utilize Citrix Presentation Server and Citrix Access Gateway to significantly increase the security and performance of the ACL and AS2 applications currently deployed to the auditors. Currently, auditors in the field are copying all data to the local computer to use their applications effectively. This represents a considerable security risk as application data is not encrypted and sensitive data could be compromised.
Objectives	Utilizing Citrix Presentation Server will allow the Office of the State Auditor to install these applications on secure servers in the data center and keep all sensitive data in the data center as well. Thus, in the event of computer theft or loss there will be no data on the computer that can be compromised. The Office of the State Auditor would also like to implement Citrix Access Gateway to improve security of the infrastructure. Citrix Access Gateway, an SSL-VPN solution, will encrypt all application traffic between the client computer and the data center using industry standard 128-bit SSL encryption. Citrix Access Gateway will also be utilized to enhance the security of the infrastructure by determining the level of access to applications and other functions (i.e. copy and paste, printing, saving to local drives, etc.) necessary for the user given their access scenario.
Time Frame	Fiscal Year 2007
Agency Relationships	Plan Driver 2.C.1 (ESAP) Plan Driver 2.C.5 (Air Defense)
Statewide Relationships	
Resources Involved	HR: Network Specialist Technology Support Specialist
Costs	The Office of the State Auditor would like to conduct a pilot to test the feasibility of deploying these applications on Citrix Presentation Server and test the functionality of Citrix Access Gateway. This pilot will require a two week engagement with Citrix Consulting to fully implement the solution. The cost of the two week pilot will be $40,000 plus travel & expenses.

Initiative: Voice over IP/Unified Messaging	**Primary Plan Driver: 2.C.6** (Infrastructure Assets – Improved communications) **Priority: 13**
Summary	Currently, Auditors working in the field (mobile workers) are not always given appropriate and/or confidential access to telephone service. OSA would like to improve communications between home and field offices by investigating VoIP options.
Objectives	• Improved communications and productivity while reduced costs (long

	distance charges, cellular phone charges) • Provide access to critical personnel and information from anywhere, with a single phone number • Provide soft phones that can operate as a primary desktop phone, supplementary phone, or field phone • Improve telephone security by making use of encrypted and secured IP data networks (anytime/anywhere secure access)
Time Frame	Fiscal Year 2007
Agency Relationships	Plan Driver 1.A (Audit Watch – improved office efficiency) Plan Driver 2.C.3 (Infrastructure Assets – Switch Replacement) Plan Driver 2.C.7 (Infrastructure Assets – Improved security for field auditors)
Statewide Relationships	
Resources Involved	HR: Network Specialist Technology Support Specialist
Costs	$30000 Increased Bandwidth: $10968 monthly recurring

Initiative: Inventory Control/ Asset Management (Iwise)	**Primary Plan Driver: 2.D.4** (Operations/IT Management – inventory/asset management) **Priority: 14**
Summary	Currently, there is no centrally managed computer hardware/software Asset management and Inventory solution. OSA spends a considerable amount of time manually updating and verifying computer asset information. OSA would like to investigate and implement ITS approved Assets Management and Inventory Control (IWise) software
Objectives	• Improve Infrastructure Assets Management and Inventory Control accuracy • Reduce costs associated with IT Asset and Inventory control
Time Frame	Fiscal Year 2007
Agency Relationships	Plan Driver: 2.D.X (Operations/IT Management – all 7 requirements)
Statewide Relationships	ITS Implementation of IWise ITS Asset Management
Resources Involved	HR: Technology Support Specialist
Costs	$15000 (primarily as a portion of resource use –tasks and their completion will be considered as regular and expected duties.)

Initiative: Beacon Project	**Primary Plan Driver: 2.A.3** (Current Projects – Beacon) **Priority:15**
Summary	Statewide HR/Payroll
Objectives	• Allow the State to operate as a seamless enterprise • Enhance the State's buying power • Provide better access to information for improved decision making
Time Frame	Q1 2006 – Q4 2008

Agency Relationships	Plan Driver 2.A.1 (Current Projects – Data Warehousing SAS) Plan Driver 2.B.4 (Current Applications – TRS)
Statewide Relationships	Beacon is a statewide initiative
Resources Involved	HR: Business and Technology Applications Specialist
Costs	$15000 (primarily as a portion of resource use –tasks and their completion will be considered as regular and expected duties.)

Initiative: Electronic Publishing System	**Primary Plan Driver: 2.B.1** (Current Applications – EPS) **Priority: 16**
Summary	The Electronic Publication System (EPS) is an asp system designed and developed by OSA to help publish Audit Reports and News Releases to the OSA Public website. In addition, EPS allows interested parties to sign up for reports that meet their selection criteria. Audit reports are automatically distributed to registered users when released.
Objectives	Current plans are to maintain and enhance system functions as required to conform to changing customer requirements and technological advancements.
Time Frame	Ongoing
Agency Relationships	Plan Driver 1.A (Audit Watch – office efficiency) Plan Driver 1.B.2 (Publish and distribute Audit reports) Plan Driver 2.C.4 (Infrastructure Assets –MS EA – SQL Server, IIS and Share Point)
Statewide Relationships	
Resources Involved	HR: Business and Technology Applications Specialist
Costs	$15000 (primarily as a portion of resource use –tasks and their completion will be considered as regular and expected duties.)

Initiative: Time Reporting System	**Primary Plan Driver: 2.B.4** (Current Applications – TRS) **Priority17**
Summary	The Time Reporting System (TRS) is an application designed and developed by OSA to provide time reporting and management for all OSA employees. In addition, TRS provides billing information for cost recovery.
Objectives	Current plans are to maintain and enhance system functions as required to conform to changing customer requirements and technological advancements.
Time Frame	Ongoing
Agency Relationships	Plan Driver: 2.A.3 (Beacon project) Plan Driver 2.A.4 (SARA E-Partners) Plan Driver 2.C.4 (Infrastructure Assets –MS EA – SQL Server, IIS and Sharepoint)
Statewide Relationships	This application will be enhanced/replaced by the statewide Beacon project.
Resources Involved	HR: Business and Technology Applications Specialist
Costs	$15000 (primarily as a portion of resource use –tasks and their completion will be considered as regular and expected duties.)

Initiative: Remote Deployment of Desktop Services	**Primary Plan Driver: 2.B.3** (current applications – Remote Deployment) **Priority:18**
Summary	Remote Deployment of ACL and AS2 utilizing WINbatch and patch link server. ACL and AS2 are mission critical vendor supplied applications for performing audits.
Objectives	• To improve capacity for updating and installing critical applications throughout the state • Eliminate costly travel costs associated with updating critical applications • Improve security by ensuring critical applications are kept up to date with security patches
Time Frame	Ongoing
Agency Relationships	Plan Driver 1.A (Audit Watch – Improved office efficiency)
Statewide Relationships	
Resources Involved	HR: Technology Support Specialist
Costs	$5000 (primarily as a portion of resource use –tasks and their completion will be considered as regular and expected duties.)

Initiative: Risk Assessment Updates	**Primary Plan Driver: 3.1** (Information Security Assessment updates) **Priority: 19**
Summary	To modify OSA IT systems, resources, policies and procedures so they conform to industry best practices as detailed in the Information Security Assessment Produced for OSA by Symantec.
Objectives	To ensure OSA eliminates or limits the number of security vulnerabilities with regards to six key IT resource areas: • Security Policy • Network Architecture • Network Vulnerability • Secure Build • Wireless Site
Time Frame	July 2006- June 2007
Agency Relationships	Plan Drivers 2.D.4 (Operations/IT Management – improved inventory/asset management) Plan Driver 2.D.6 (Operations/IT Management - Improved Security management) Plan Driver 2.D.7 (Operations/IT Management - Improved disaster recovery and BCP planning)
Statewide Relationships	
Resources Involved	HR : Technology Support Analyst Technology Support Specialist Business and Technology Applications Analyst Business and Technology Applications Specialist

	Business and Technology Applications Specialist Network Specialist
Costs	All members of the MIS staff will be involved in initiatives under this project. Tasks will be included in staff members yearly work plans and their completion will be considered as regular and expected duties.

Initiative: Office Computer/ Laptop Computer Refresh	**Primary Plan Driver: 2.C.1** (Infrastructure Assets – PC Refresh) **Priority: 20**
Summary	Out dated computer hardware is to be replaced with current technology. Currently there are 84 desktop/laptop computers that are scheduled for replacement.
Objectives	• To maintain a level of technology to ensure reliable and secure computer usage • Mitigate the risk of obsolete computer hardware
Time Frame	1st quarter 2007
Agency Relationships	Plan Driver 1.A (Audit Watch, Improved office efficiency) Plan Driver 2.D.4 (Operations/IT Management – Improved Inventory/Asset management) Plan Driver 2.D.5 (Operations/IT Management - Internal Agency consolidation plans)
Statewide Relationships	Statewide PC/Laptop bulk purchases Desktop Standardization
Resources Involved	HR - Technology Support Analyst - Technology Support Specialist
Costs	$109200

Appendix A – IT Initiatives / IT Resources (HR) Matrix

	CIO	Tech. Support Analyst	Tech Support Specialist	Bus. & Tech Appl. Analyst	Bus. & Tech Appl. Specialist	Bus. & Tech Appl. Specialist	Network Specialist	* Security/ Bus. Continuity Specialist *
Initiative: Non-Governmental Organizations	X				X			X
Initiative: Data Mining/Business Intelligence	X					X		
Initiative: Infrastructure Upgrades	X						X	
Initiative: MS Enterprise Agreement/ Server Upgrde	X		X		X		X	X
Initiative: Security/ Business Continuity Specialist	X							X
Initiative: IT Salary Adjustment	X							
Initiative: AirDefense (Wireless Security)	X						X	
Initiative: ESAP and OSA End to End Encryption	X						X	
Initiative: Vital Services Suite	X						X	
Initiative: State Auditors Resource Area	X			X	X			
Initiative: Cisco Support	X						X	
Initiative: Terminal Services	X		X				X	X
Initiative: Voice over IP/Unified Messaging	X		X				X	
Initiative: Inventory Control/Asset Management	X	X	X					X
Initiative: Beacon Project	X					X		
Initiative: Electronic Publishing System	X					X		X
Initiative: Time Reporting System	X			X	X			X
Initiative: Remote Deployment of Desktop	X	X	X					
Initiative: Risk Assessment Updates	X	X	X	X	X	X	X	X
Initiative: Office Computer/Laptop Refresh	X	X	X					X

- Security Bus. Continuity Specialist is a proposed position.

Appendix B – IT Initiatives / Business Requirements Matrix

	1.A – Audit Watch Office Efficiency	1.B.1 NGO Reporting	1.B.2 – Publish Audit Reports	1.B.3 – Employee Communications	2.A.1 – Data Warehouse SAS	2.A.2 – Network Perf Monitor	2.A.3 - Beacon	2.A.4 – SARA E-Partners	2.B.1 - EPS	2.B.2 - NGO	2.B.3 Remote Deployment	2.B.4 - TRS	2.C.1 – Infrastructure – PC Refresh	2.C.2 – Infrastructure – ESAP	2.C.3 – Infrastructure – Switch Rpl	2.C.4 – Infrastructure – MS EA	2.C.5 – Infrastructure- Wireless Sec	2.C.6 – Infrastructure – VoIP	2.C.7 – Infrastructure –Field Secur	2.D.1 IT Mgt - ITIL	2.D.2 IT Mgt – Proj Mgt	2.D.3 IT Mgt – Appl Mgt	2.D.4 IT Mgt – Inv/Asset Mgt	2.D.5 IT Mgt – Internal Consl. Plan	2.D.6 IT Mgt – Network Monitor	2.D.7 IT Mgt – DR/BCP/COOP	3.1 – Info Sec Assessment Updt	3.2 – Salary Adjustments
Initiative: Non-Governmental Organizations	x	x			x			x		P																		
Initiative: Data Mining/Business Intelligence					P		x			X																		
Initiative: Infrastructure Upgrades						x								x	P			x										
Initiative: MS Enterprise Agreement/ Server Upgrde	x								x	x	x					P											x	
Initiative: Security/ Business Continuity Specialist																	X	x	x	x			x		x	P	x	
Initiative: IT Salary Adjustment	x																											P
Initiative: AirDefense (Wireless Security)																	P		x						x		x	
Initiative: ESAP and OSA End to End Encryption														P	x				x									
Initiative: Vital Services Suite						P									x										x		x	
Initiative: State Auditors Resource Area	x			x				P								x												
Initiative: Cisco Support														x	P										x		x	
Initiative: Terminal Services														x			X		P									
Initiative: Voice over IP/Unified Messaging	x														x			P	x									
Initiative: Inventory Control/Asset Management																				x	x	x	P	x	x	x		
Initiative: Beacon Project					x		P					x																
Initiative: Electronic Publishing System	x		x						P							x												
Initiative: Time Reporting System							x	x				P				x												
Initiative: Remote Deployment of Desktop	x										P																	
Initiative: Risk Assessment Updates																							x		x	x	P	
Initiative: Office Computer/Laptop Refresh	x												P										x	x				